International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 3 Mar 2022, pp: 722-727 www.ijaem.net ISSN: 2395-5252

Efficient Management of Electronic Health Record system by using cloud computing

Shubham Ingle, Anisaaara Nadaph
Department of Computer Engineering Trinity College of Engineering and Research
Department of Computer Engineering Trinity College of Engineering and Research

Submitted: 10-03-2022 Revised: 21-03-2022 Accepted: 23-03-2022

ABSTRACT— Cloud-based Electronic Health Record (CB-EHR) systems have much potential to facilitate the maintenance of individual health records. Protection and privacy are two of the main obstacles to the widely adopted CB-EHR systems. The present paper considers a Multi-source CB-EHR scheme whereby individual data proprietors can upload their personal health data into an untrusted public cloud by multiple data providers, including hospitals and doctors. Health data are provided in encrypted form in order to ensure data protection, and every provider provides encrypted data indexes to support encoded data queries. The PPIA system offers the possibility to combine encrypted data indexes from several data providers without being familiar with the index information. PPIA provides an efficient and privacy safeguarded processing of the database by enabling a data user to submit a single data query that the cloud can process without the knowledge of the query material via encrypted data from all relevant data providers. We also propose a more efficient scheme to support hierarchical data providers' data queries. The effectiveness and efficiency of PPIA were shown through extensive studies and real data sets experiments.

Index Terms—EHR, cloud storage, privacy-preserving, security.

I. INTRODUCTION

With the exponential rise in global knowledge, the cloud services industry has expanded without precedents. Many cloud suppliers, including Am-azon, GOOGLE, Alibaba, Huawei, and Microsoft, are launching cloud services and products. People begin to deliver their massive data storage tasks to cloud service providers (CSPs). It does not restrict them anymore to a small amount of storage and computer resources. A practical and high quality example of cloud storage is supporting the electronic health records (CB-EHR), a system that collects information about patients' digital health, from many organisations, like the United States' National Coordinator for Health Information Technology. Patient EHRs are available on the work station or mobile device and can be later updated. In order to assiste patients in greater treatment, to help scientists study and re-evaluation diseases, and to support government health services foreseen, track and potentially deter infectious disease outbreaks, various medical institutions can exchange patients with EHRs uploaded into the cloud. As the Cloud Service Provider (CSP) is an independent management agency, consumers literally abandon absolute control of their EHRs. This poses safety issues when the activities are outsourced. For instance, cloud servers will return fake results for a variety of reasons, including cloud malfunction and a hacker attack. The incorrect return value may affect all aspects of the medical system significantly. Consequently, the main problem with EHR is how to check the server correctly each time.

Cloud-based electronic health record systems (CB-EHR) now rise for a few days. Three traditional CB-EHR systems are available: data owners, data providers and a cloud server. In the CB-EHR framework both patient and hospital data owners and data providers are specified. Data owners can download their EHRs directly to the cloud by provider data providers. A more detailed overview everywhere, better prepared for medical meetings or unexpected emergencies, and an improved picture of personal health and fitness targets, is provided by the CB-EHR Framework for data owners. Throwing out the CB-PHR framework to provide improved medical services, through sharing, collaboration and involvement of patients in various ways.

In this paper we propose a highly effective CB-EHR system to ensure good privacy. Each data owner in our system enabled several data providers to deliver encrypted health records and information

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 3 Mar 2022, pp: 722-727 www.ijaem.net ISSN: 2395-5252

to the cloud server. Our system is different from previous work in two desirable features. First of all, each data provider from the same data owner uses a special, symmetrical key to encrypt the data index, which resists a single point. Second, not every data owner needs to manage keys with each health provider and can send an encrypted query to the cloud server to check encrypted data from all its data providers. The second function is very effective for query processing.

A. MOTIVATION

1) Health play a crucial role in every individual's life and safety of health records is necessary.
2) The specific and sensitive attributes value of our CB-EHR system is used in access policy.
3) The system is used for the efficient development of an intelligent health care system.
4) Data sharing by users other than all information may be shared and other information may be shared in this scheme.

5) If even patients do not receive reports, our patient or user will not be able to receive a file or a report in a hospital or laboratory.
6) Easy to use, easy to get application reports.

II. REVIEW OF LITERATURE

1) The new period of diverse well-being introduced by a wide range of routine processing and mobile exchanges has provided governments and organisations with open doors to re-examine their idea of human services. In all this, the overall urbanisation process speaks of a substantial test and considers urban areas which must be constructed productively and humanely to furnish higher populations and administrative subjects. The two patterns caused mobile well-being and brilliant urban environments. The new idea of a shrewd well-being is presented in this article, which is a conscious supplement to diverse well-being in brilliant urban communities. We provide a diagram of the fundamental learning fields that are involved in the construction of this new concept. We also look into the fundamental problems and openings that s-Health proposes and share a view to further study[1].

2) Distributed computing is a key component of the Internet of Things foundation (IoT). A great deal of cooperation with changing qualitative needs is needed to help. Consequently, the quality of administration will be a critical distinction between cloud providers. Cloud suppliers should offer incomparable administrations that meet the wishes of their customers to get away from their rivals. A quality model can be used to talk about the nature of suppliers, measure them and examine them, with the aim of building a common understanding between cloud partners. We take an administrative view in this document and develop a quality model for cloud administrations known as CLOUDQUAL. It is a model with measurements and quality that generally targets cloud management. CLOUDQUAL consists of six quality measures that are emotionally user-friendly and objective: easy use, accessibility, constant quality, responsiveness, security, and flexibility. We carry out exact contextual analysis on three storage mixtures to demonstrate the viability of CLOUDQUAL. Results show that CLOUDQUAL can evaluate its quality. We approve CLOUDQUAL in accordance with standard criteria to show its soundness and to show that it can separate the quality of administration[2].

3) Fine-grained access to encrypted data attribue-based encryption." Since the information is progressively sensitive and is shared by outsiders on the Internet, information needs to be shared at these locations. One disadvantage is that information can be shared very well only at a gross grain level (i.e., giving another gathering your private key). For fine-grained information-sharing, we build another crypto-system that we call key policy attribute-based encryption (KP-ABE). Figures are marked with sets of characteristics in our crypto-system and private keys are related to access structures that control what a customer can scramble messages. We demonstrate the materiality of our development for sharing log data and for communicating encryption. We are developing private keys that subsume HII-based encryption (HIBE)[3]. Our development supports [3].

4) We present a different type of IDE (IBE) plot we call a Fuzzy IDE. Fuzzy IDE. We see a way of life as an illustrative set of features in Fuzzy IBE. A Fuzzy IBE plot takes into account a private keypad, 0, if the characters are close to one another, as estimated by the "set cover," delete metrics, to unscrew a personality screwing figure content. A Fuzzy IBE plan can be linked with a feasibility to encrypt using biometric character contributions; a Fuzzy IBE plot's error-resistance property correctly takes the use of biometric personalities into account and they are innately criticised every time they are tested. We also show that Fuzzy-IBE can be used to use some type of encryption based upon property [4].

5) Distributed computing is the latest in the vision of registering as a utility envisaged since a few years ago. The cloud provides advantageous on-demand

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 3 Mar 2022, pp: 722-727 www.ijaem.net ISSN: 2395-5252

access by organising an integrated pool of configurable, highly efficient registration assets[5].

6) We present a PDP model that allows an untrusted server to provide a customer who has provided information to confirm that the first information is available without recovery. The model produces probabilistic proof of ownership by testing arbitrary square arrangements on the server, which definitely reduces I/O costs. In order to confirm the proof, the client maintains a consistent measure of metadata[6].

7) We characterise and study evidence of recovery in this paper (PORs). A POR plot enables the file/backup management (prover) to give a compact confirmation that a client (verifier) will be able to retrieve objective F document, namely that the file holds and reliably transmits data to the customer to fully recover F [7].

8) By using the cloud storage, customers can store data remotely and enjoy top-notch applications and administrations on request from a shared pool of configurable processing equipment without the weight of the storage and maintenance of information in the vicinity[8].

9) A data storage centre must show a verifier in an evidence-of-recovery system that all data of a customer is actually stored. The key challenge is to build efficient and testamentally secure systems—the client data from any prover who carries out a verification check should therefore be extracted. In this article, we present in the strongest model, the one of Juels and Kaliski [9], the first proof of recovery schemes with full evidence of security against arbitrary adversaries.

III. SYSTEM OVERVIEW

In Our System, we have proposed a cloud-based data integrity audit scheme that supports data sharing with hidden sensitive information. When Doctor shares data with User that file with Admin and Admin in binary format converts, Doctor will then upload the data into the cloud with the user and convert it into homogeneous encryption and into block level again. Download the data in our application doctor with cloud.

In the system, there are four roles, including the physician, administrative author and the patient and the researcher and First, the system physician, upload the report, depending on their choice of user and researcher. Use Specialized Algorithms to convert data to Binary format. The data is stored on a second level encryption, for example called the content level encryption and copying into block level, after being converted to a Binary Bonal Cloud Server Provider. Private key is generated and stored in that cloud server provider admin. Search the report by user and then search by patient ID, first audit and authorised report and again manage the user Download the report by private key.

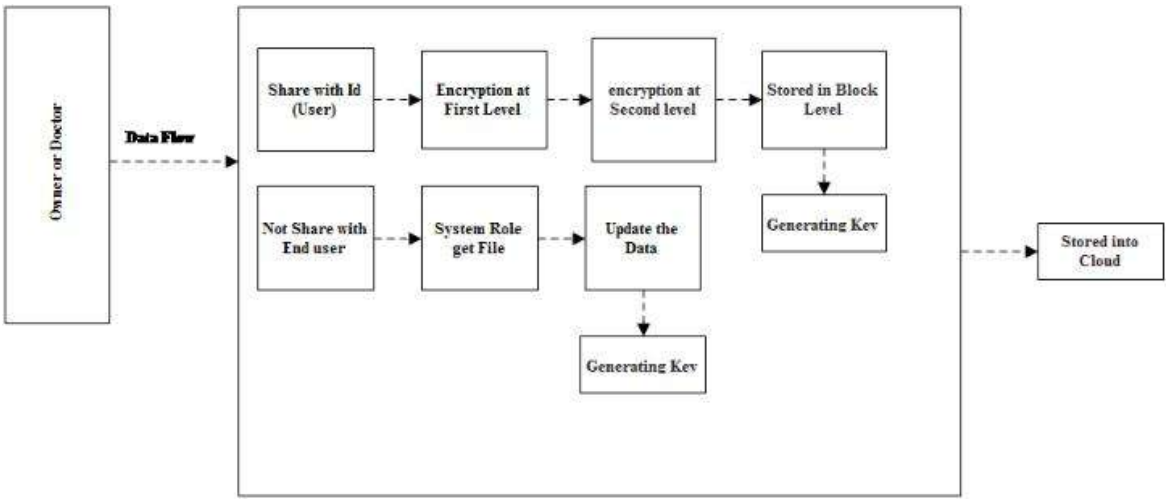

Fig. 1. Proposed System Architecture

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 3 Mar 2022, pp: 722-727 www.ijaem.net ISSN: 2395-5252

A. Algorithms

1. Generation of Block B

1) for i=0;i¡=k;i++ do

2) for j=0;j¡=k;j++ do

3) if j==0 then

4) Bi,j=0; else

5) bi,j=ik+j;

6) end if

7) end for

8) end for

9) for i=k+1 ;i¡=k +k ;i++ do

10) for j=0;j¡k ;j++

11) j==0 then

12) Bi,j=[(i-1)/k +1]

13) Else

14) Bi.k=jk+1 +Mod k+1(i-j+(j-1)[i-1]/k+1)

15) End if

16) End for

17) End for

2. Re-construction of B

1) E0=B0; Steps 1

2) For t=1;t¡=k+1;t++ do

3) Et=Btk+1 Steps 2

4) Btk=[Flag]=1;

5) Eet,1=B[Et,t/ K] steps 2

6) Btk+1[flag]=1

7) End for

8) For i=k+1 ;i¡k+1; i++ do

9) If Bi[Flag]!=1 then

10) Ebi[i+1/K]=Bi steps 3

11) End if

12) End For

3. AES Algorithms 1) Input: 2)128 bit /192 bit/256 bit input(0,1)
3)secret key(128 bit)+plain text(128 bit).

4) Process:

5)10/12/14-rounds for-128 bit /192 bit/256 bit input

6)Xor state block (i/p)

7)Final round:10,12,14

8)Each round consists:sub byte, shift byte, mix columns, add round key.
9)Output:

10)cipher text(128 bit)

B. Mathematical Model

Let us consider S as a system for EHR management system

on cloud.

S=

INPUT:

Identify the inputs

F= f1, f2, f3 ....., FN— F as set of functions to execute

commands.

I= i1, i2, i3—I sets of inputs to the function set

O= o1, o2, o3.—O Set of outputs from the function sets, S=I,F,O

I = file uploaded by the user

O = Output i.e. file already present or not, data security F = Functions implemented to get the output Space Complexity:

The space complexity depends on Presentation and visualization of discovered patterns.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 3 Mar 2022, pp: 722-727 www.ijaem.net ISSN: 2395-5252

More the storage of data more is the space complexity.

Time Complexity:

Check No. of patterns available in the datasets= n

If (n(1)) then retrieving of information can be time consuming.

So the time complexity of this algorithm is O (nˆn).

= Failures and Success conditions. Failures:

1. Huge database can lead to more time consumption to get the information.
2. Hardware failure.
3. Software failure. Success:
1. Search the required information from available in Datasets.

2. User gets result very fast according to their needs.

IV. SYSTEM ANALYSIS AND RESULT

In this subsection, our System evaluates the performance of the proposed scheme by several experiments. System runs these experiments on a window machine with an Intel Pentium 2.30GHz processor and 8GB memory. All these experiments use Java programming language with the various encryption algorithms such as AES, Blowfish. In our experiments, System first Install required Software.

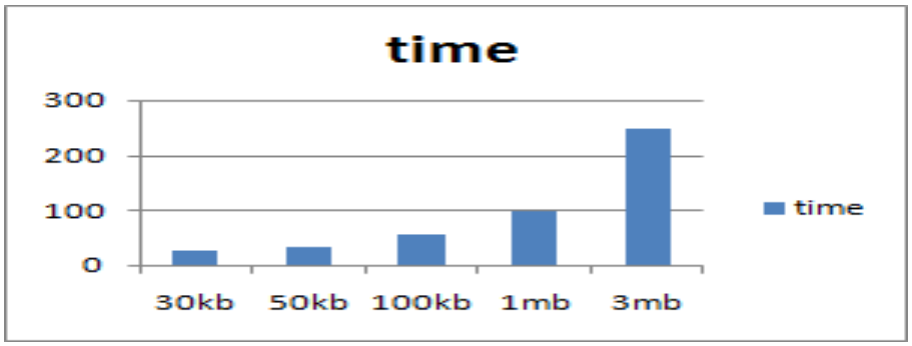

Figure 1: Shows file size on x axis and time (MS) to upload on Y-axis

Index Number	File size	Time in ms(AES)	Time in ms(Blowfish)
1	30kb	30	28
2	50kb	35	31
3	100kb	60	58
4	1mb	100	93
5	3mb	250	245

Table 1: Show File Size and Time to Upload

V. CONCLUSION

The theme of multifunctional privacy protection in the cloud-based EHR setting is discussed in this paper. Our proposed PPIA mechanism offers a stable, easy and effective way to authenticate data owners to query data from several providers compared to previous projects. To perform the query successfully. We are proposing a new Privacy Save Integrity Audit to reduce data owners' query cost and allow a cloud server to query them safely. We suggest an improved method of multi-order encryption to fulfil the hierarchically authenticated request to make our model more realistic. In order to prove that our systems are safe, we also use strict safety controls. Finally, we demonstrate that the PPIA mechanism is computer powerful by implementing our programmes and running into a real dataset.

REFERENCES

[1] Solanas, C. Patsakis, M. Conti, I. S. Vlachos, V. Ramos, F. Falcone, O. Postolache, P. A. Perez´-Mart´ınez, R. Di Pietro, D. N. Perrea et al., "Smart health: a context-aware health paradigm within smart cities," IEEE Communications Magazine, vol. 52, no. 8, pp. 74-81, 2014.

[2] Y. Yuehong, Y. Zeng, X. Chen, and Y. Fan, "The internet of things in healthcare: An overview," Journal of Industrial Information Integration, vol. 1, pp. 3-13, 2016.

[3] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233-2243, 2014

[4] X. Zheng, P. Martin, K. Brohman, and L. Da Xu, "Cloudqual: a quality model for cloud services," IEEE transactions on industrial informatics, vol. 10, no. 2, pp. 1527-1536, 2014.

[5] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Proceedings of International Conference on the Theory and Applications of Crypto-graphic Techniques (EUROCRYPT'08), 2008, pp. 146-162.

[6] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan. 2012.

[7] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 598–609.

[8] A. Juels and B. S. Kaliski, Jr., "Pors: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 584–597.

[9] H. Shacham and B. Waters, "Compact proofs of retrievability," J. Cryptol., vol. 26, no. 3, pp. 442–483, Jul. 2013.v